CHAPTER 10

STORAGE AND DESTRUCTION

10-1 BASIC POLICY

1. Commanding officers shall ensure that all classified information is stored in a manner that will deter or detect access by unauthorized persons. Classified information which is not being used or not under the personal observation of cleared persons who are authorized access shall be stored per this chapter. To the extent possible, limit areas in which classified information is stored and reduce current holdings to the minimum required for mission accomplishment.

2. Weapons or sensitive items, such as money, jewels, precious metals, or narcotics shall not be stored in the same security containers used to store classified information.

3. There shall be no external markings revealing the classification level of information being stored in a specific security container, vault, or secure room. Priorities for emergency evacuation and destruction shall not be marked or posted on the security container. This does not preclude placing a mark or symbol on the security container for other purposes or applying decals or stickers required by the DCI for security containers used to store or process intelligence information.

4. Report to the CNO (N09N3) any weakness, deficiency, or vulnerability in any equipment used to safeguard classified information. Include a detailed description of how the problem was discovered and the measures taken to mitigate it, and classify per chapter 4 of this regulation, if applicable.

10-2 STANDARDS FOR STORAGE EQUIPMENT

The GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and destruction of classified information. Reference (a) describes acquisition requirements for physical security equipment used within the DoD.

10-3 STORAGE REQUIREMENTS

1. Classified information not under the personal control or observation of an appropriately cleared person shall be guarded or stored in a locked GSA-approved security container, vault,

modular vault, or secure room (open storage area constructed per exhibit 10A) as follows:

a. Store Top Secret information by one of the following methods:

(1) In a GSA-approved security container with one of the following supplemental controls;

(a) The location housing the security container shall be subject to continuous protection by cleared guard or duty personnel;

(b) Cleared guard or duty personnel shall inspect the security container once every 2 hours;

(c) An Intrusion Detection System (IDS) with personnel responding to the alarm within 15 minutes of the alarm annunciation;

(d) Security-in-Depth when the GSA-approved security container is equipped with a lock meeting Federal Specification FF-L-2740; or

(e) In either of the following: (1) An open storage area (secure room) or vault which is equipped with an IDS with personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-in-Depth or a 5-minute alarm response if it is not.

b. Store Secret information by one of the following methods:

(1) In the same manner prescribed for Top Secret;

(2) In a GSA-approved security container, modular vault, or vault without supplemental controls; or

(3) In either of the following: (1) Until 1 October 2002, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved security container secured with a rigid metal lock-bar and a GSA-approved padlock, or (2) An open storage area (secure room) with one of the following supplemental controls:

(a) The location housing the open storage area is subject to continuous protection by cleared guard or duty personnel;

(b) Cleared guard or duty personnel shall inspect the area once every 4 hours; or

(c) An IDS with response time within 30 minutes of alarm annunciation.

(4) Commands are encouraged to replace non-GSA-approved cabinets with GSA-approved security containers as soon as feasible prior to the mandatory replacement date of 1 October 2002. New lock-bar cabinets shall not be fabricated from either existing or new containers, nor shall any existing lock-bar container that was not previously used for the protection of classified information be put into use for that purpose.

c. Store **Confidential** information in the same manner prescribed for Top Secret or Secret **except** that supplemental controls are not required.

2. Under field conditions during military operations, the commanding officer may require or impose security measures deemed adequate to meet the storage requirements in paragraphs 10-3.1a through c, commensurate to the level of classification.

3. Reference (b) governs the requirements for storing classified ordnance items too large to store in GSA-approved containers.

4. Storage areas for bulky material containing Secret or Confidential information may have access openings secured by GSA-approved combination padlocks (Federal Specification FF-P-110 Series), or high security key-operated padlocks (MIL-P-43607). If these storage requirements cannot be met afloat or on board aircraft, Secret or Confidential information may be stored in a locked container constructed of metal or wood (such as a foot locker or cruise box) secured by a GSA-approved padlock meeting Federal Specification FF-P-110. The area in which the container is stored shall be locked when not manned by U.S. personnel and the security of the locked area checked once every 24 hours.

5. Commanding officers shall establish standard operating procedures to include screening points, in order to ensure that all incoming mail, including bulk shipments, are secured until a determination is made as to whether or not they contain classified information. Overnight storage of certain unopened mail, overnight delivery, USPS Express, first class, certified, or registered mail (all of which could contain classified information), shall be safeguarded per chapter 7, paragraphs 7-3 through 7-5 and reference (c).

10-4 PROCUREMENT OF NEW STORAGE EQUIPMENT

1. If new security storage equipment is needed, procure it from the GSA Federal Supply Schedule. However, prior to procuring new storage equipment, conduct a physical security survey of existing equipment and review classified records on hand. Coordinate with the records manager to determine if it is feasible to use available equipment or to retire, return, declassify, or destroy a sufficient volume of records on hand to make the needed security storage space available. Promptly report excess containers (if any) to property disposal and fulfill requirements for added equipment through property disposal when that is more cost effective.

2. Security containers conforming to Federal Specifications have a Test Certification Label on the inside of the control locking drawer. Containers manufactured after February 1962 will also be marked "General Services Administration Approved Security Container" on the outside of the top drawer. Specifications have been developed for 8 classes of security containers (Classes 1, 2, 3, 4, 5, 6, 7, and 8.) However, only 6 classes (Classes 1, 2, 3, 4, 5, and 6) are approved for storage of classified information, and only Classes 5 and 6 are currently on the GSA schedule. The removal of approved security containers from GSA schedule does not negate the approval. Previously approved GSA containers may still be used to store classified information provided they meet the original level of integrity and have not had the Test Certification Label removed for cause.

10-5 REMOVAL OF SECURITY CONTAINERS

Security containers that have been used to store classified information shall be inspected by appropriately cleared personnel before removal from protected areas or before unauthorized persons are allowed access to them. The inspection shall ensure that no classified information remains within.

10-6 SHIPBOARD CONTAINERS AND FILING CABINETS

1. Shipboard containers shall conform to DON standards for durability, size, weight, maintainability, and safety. Non GSA-approved filing cabinets and safe lockers of various sizes and shapes are available for use. These cabinets and safe lockers are designed and constructed according to various hull type drawings and ship drawings, and are equipped with mechanical Group 1R combination locks.

2. The requirement to store Secret and Confidential information in these types of locked containers also includes implementing supplemental security measures such as continuous operations, or locking the surrounding area when not manned by U.S. personnel with the locked area checked every 24 hours.

3. New ship construction requirements shall include GSA-approved security containers and comply with the storage requirements of this regulation.

4. Mechanical locks on existing shipboard file cabinets and safe lockers do not have to be replaced with locks meeting Federal Specification FF-L-2740.

10-7 VAULTS AND SECURE ROOMS

1. Entrances to vaults or secure rooms shall be under visual control during duty hours to prevent entry by unauthorized personnel, or equipped with electric, mechanical, or electro-mechanical access control devices to limit access. Electrically actuated locks (e.g., cipher and magnetic strip card locks) do not afford by themselves the required degree of protection for classified information and shall not be used as a substitute for the locks prescribed in paragraph 10-3.

2. Periodically examine existing areas and promptly repair correctable defects. Existing approved vaults and secure rooms do not require modification to meet current standards.

3. GSA-approved modular vaults meeting Federal Specification AA-V-2737 may be used to store classified information as an alternative to vault requirements as described in **exhibit 10A**.

10-8 SPECIALIZED SECURITY CONTAINERS

1. GSA-approved field safes and special purpose one- and two-drawer light-weight security containers are intended primarily for storage of classified information in situations where normal storage is not feasible. These containers shall be securely fastened to the structure to render them non-portable or kept under constant surveillance to prevent their theft.

2. GSA-approved map and plan file containers are available to store odd-sized classified items such as computer media, maps, and charts.

10-9 NON GSA-APPROVED SECURITY CONTAINERS

Immediately remove security containers manufactured by Remington Rand from service and dispose of them under accepted safety standards. Previously approved two- and four-drawer Class 5 security containers manufactured by Art Metal Products, Inc., are no longer authorized for the protection of classified information.

10-10 RESIDENTIAL STORAGE

1. Top Secret information may be removed from designated areas for work at home during off-duty hours only as authorized by the SECDEF, the Secretaries of the Military Departments, the Combatant Commander, and the CNO (N09N).

2. Secret and Confidential information may be removed from designated areas for work at home during off-duty hours only as authorized by the CNO (N09N), a Fleet Commander in Chief, the Commander of the Naval Space Command, the Commanders of the Naval Systems Commands, the Chief of Naval Research, the Commandant of the Marine Corps, or the Commanding General of U.S. Marine Corps Forces Atlantic or Pacific.

3. A critical operational requirement shall exist for consideration of such requests. A GSA-approved security container shall be furnished for residential storage. Additionally, Top Secret information shall be protected with an IDS or comparable supplemental controls. Written procedures shall be developed to provide for appropriate protection of the information, to include a record of the classified information that is authorized for removal.

10-11 REPLACEMENT OF COMBINATION LOCKS

1. Exhibit 10B is the priority list for replacing existing mechanical combination locks with locks meeting Federal Specification FF-L-2740. The mission and location of the command, the classification level and sensitivity of the information, and the overall security posture of the command determines the priority for replacement of existing combination locks. All system components and supplemental security measures including IDS, automated entry control subsystems, video assessment subsystems, and level of operations shall be evaluated

when determining the priority for replacement of security equipment. Priority 1 requires immediate replacement.

2. New purchases of combination locks shall conform to Federal Specification FF-L-2740. Existing mechanical combination locks shall not be repaired. They shall be replaced with locks meeting Federal Specification FF-L-2740.

10-12 COMBINATIONS

1. Only personnel who have the responsibility and possess the appropriate clearance level shall change combinations to security containers, vaults and secure rooms. Combinations shall be changed:

a. When first placed in use;

b. When an individual knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock;

c. When a combination has been subjected to compromise; or

d. When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

2. The combination of a container, vault, or secure room used for the storage of classified information shall be treated as information having a classification equal to the highest category of the classified information stored therein. Mark any written record of the combination with the appropriate classification level.

3. Maintain a record for each security container, vault, or secure room showing the location of each, the names, home addresses, and home telephone numbers of all persons having knowledge of the combination. Use SF 700, "Security Container Information," for this purpose.

a. Place Part 1 of the completed SF 700 on an interior location in security containers, vault or secure room doors. Mark Parts 2 and 2A of the SF 700 to show the highest classification level and any special access notice applicable to the information stored within. Store Parts 2 and 2A in a security container other than the one to which it applies. If

necessary continue the listing of persons having knowledge of the combination on an attachment to Part 2.

b. If a container is found unsecured, unattended, or shows evidence of unauthorized entry attempt, notify the appropriate official.

10-13 KEY AND PADLOCK CONTROL

1. Commanding officers shall establish administrative procedures for the control and accountability of keys and locks whenever high security key-operated padlocks are used. The level of protection provided each key shall be equivalent to the highest classification level of information being protected by the padlock.

2. Reference (d) makes unauthorized possession of keys, keyblanks, keyways, or locks adopted by any part of the DoD for use in the protection of conventional arms, ammunition or explosives (AA&E), special weapons, and classified equipment a criminal offense punishable by fine or imprisonment up to 10 years, or both.

3. Reference (e) governs key security and lock control used to protect classified information.

4. Reference (b) governs controls and security of keys and locks used for AA&E.

10-14 SECURING SECURITY CONTAINERS

When securing security containers, rotate the dial of combination locks at least four complete turns in the same direction, and check each drawer. In most locks, if the dials are given only a quick twist, it is possible to open the lock merely by turning the dial back to its opening position.

10-15 REPAIR, MAINTENANCE, AND OPERATING INSPECTIONS

1. Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who have been the subject of a trustworthiness determination per reference (f) or, who are continuously escorted.

a. With the exception of frames bent through application of extraordinary stress, a GSA-approved security container

manufactured prior to October 1991 (identified by a silver GSA-label with black lettering affixed to the exterior of the container) is considered restored to its original state of security integrity as follows:

(1) If all damaged or altered parts (e.g., locking drawer, drawer head, or lock) are replaced with new or cannibalized parts; or

(2) If a container has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, the replacement lock shall meet Federal Specification FF-L-2740; the drilled hole shall be repaired with a tapered case-hardened steel rod (e.g., dowel, drill bit, or bearing) with a diameter slightly larger than the hole and of such length that when driven into the hole there remains, at each end of the rod, a shallow recess not less than 1/8 inch nor more than 3/16 inch deep to permit the acceptance of substantial welds; and the rod is welded on the inside and outside surfaces. The outside of the drawer head shall be puttied, sanded, and repainted so no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts.

b. In the interest of cost efficiency, the procedures identified in paragraph 10-15a(2) shall not be used for GSA-approved security containers purchased after October 1991 (identified by a silver GSA label with red lettering affixed to the outside of the container control drawer) until it is first determined whether warranty protection still applies. To make this determination, contact the manufacturer and provide the serial number and date of manufacture of the container. If a Class 5 security container is under warranty, use the procedures described in the Naval Facilities Engineering Service Center (NFESC) Technical Data Sheet (TDS) 2000-SHR, "Neutralizing Locked-Out Containers," to neutralize a lock-out. If a Class 6 security container is under warranty, use the procedures described in the NFESC TDS 2010-SHR, "Red Label Class 6 Security Container Opening Procedures," to neutralize a lock-out.

2. GSA-approved containers which have been drilled in a location or repaired in a manner other than described in paragraph 10-15a(2) are not considered restored to their original state of security integrity. Remove the "Test Certification Label" on the inside of the locking drawer and the "General Services Administration Approved Security Container" label on the outside of the top drawer of the container. Place a permanently marked notice to this effect on the front of the container. As a

result, these containers may be used to store only unclassified information.

3. When repair results are visible and could be mistaken for marks left in an attempt to gain unauthorized entry to the container, stamp a registration mark in the metal of the container and post a label inside the locking drawer stating the details of the repair. Use exhibit 10C to record the history of the security equipment to reflect the operating problems, the type of maintenance, the date repaired/inspected, the name and company of the technician, the name of the command, and the certifying official. Retain this record for the service life of the security container/vault door.

4. External modification of GSA-approved security containers to attach additional locking devices or alarms is prohibited.

10-16 ELECTRONIC SECURITY SYSTEM (ESS)

1. An ESS consists of one or a combination of the following subsystems:

    a. IDS;

    b. Closed Circuit Television (CCTV); and

    c. Access Control System (ACS).

2. An IDS monitors electronic sensors designed to detect, not prevent, an attempted intrusion. Some of the major phenomena these sensors are designed to detect are movement, changes in heat sources, door openings, and sound changes. A CCTV system is designed to assess, view areas, or detect an intrusion. Some of the major components of a CCTV system are cameras, thermal images, switchers, and video motion detectors. An ACS system is designed to help control access to spaces. Major ACS components consist of card reader devices, biometrics, and hand geometry components and the computers to control them.

3. An ESS provides additional controls at vital areas as insurance against human or mechanical failure. The use of an ESS in the protective program of a command may be required because of the critical importance of a command's mission, design, layout, or location of the facility. In some instances, their use may be justified as a more economical and efficient substitute for other protective measures.

4. Commercial IDSs used on storage containers, vaults, modular vaults, and secure rooms shall be approved by the CNO (N09N3). Existing IDSs may continue to be used and do not need approval until upgraded or replaced.

5. Exhibit 10D provides guidance regarding IDSs and ACSs.

10-17 DESTRUCTION OF CLASSIFIED INFORMATION

1. Destroy classified information no longer required for operational purposes per reference (g). Destruction of classified information shall be accomplished by means that eliminate risk of recognition or reconstruction of the information.

2. Commanding officers should establish at least 1 day each year "clean-out" day when specific attention and effort are focused on disposition of unneeded classified and controlled unclassified information.

3. Refer to references (h) and (i) for destroying COMSEC information, reference (j) for destroying SCI, and reference (k) for destroying NATO information.

4. Refer to reference (l) for AIS storage media destruction techniques.

5. The Directorate for Information Systems Security, NSA, provides technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media and processing equipment components.

6. Obtain specifications concerning appropriate GSA-approved equipment and standards for destruction through the National Supply System (FSC Group 36, Part II).

7. Refer to exhibit 2B for emergency destruction guidelines.

10-18 DESTRUCTION METHODS AND STANDARDS

1. Various methods and equipment may be used to destroy classified information that include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing.

2. A cross-cut shredder shall reduce the information to shreds no greater than 3/64 inch wide by 1/2 inch long. Strip shredders purchased prior to 29 April 1988 may continue to be used; however, new purchases shall be cross-cut shredders.

3. Pulverizers and disintegrators must have a 3/32 inch or smaller security screen.

4. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material.

10-19 DESTRUCTION PROCEDURES

1. Commanding officers shall establish procedures to ensure that all classified information intended for destruction is destroyed by authorized means and appropriately cleared personnel. Classified information that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center.

2. Classified information shall be controlled in a manner designed to minimize the possibility of unauthorized removal and/or access. A burn bag may be used to store classified information awaiting destruction at a central destruction facility. Seal and safeguard each burn bag per this regulation until actually destroyed.

3. A record of destruction is required for Top Secret information. The use of OPNAV 5511/12, "Classified Material Destruction Report," is no longer required. Record destruction of Top Secret and any special types of classified information (if required) by any means as long as the record includes complete identification of the information destroyed and date of destruction. The record shall be executed by two witnesses when the information is placed in a burn bag or actually destroyed. Retain Top Secret records of destruction for 5 years. Records of destruction are not required for waste products containing Top Secret information.

4. Records of destruction are not required for Secret and Confidential information except for special types of classified information (see paragraphs 7-7 and 10-17).

10-20 DESTRUCTION OF CONTROLLED UNCLASSIFIED INFORMATION

1. Destroy record copies of FOUO, SBU, DoD UCNI, DOE UCNI, Sensitive (Computer Security Act of 1987), and unclassified technical documents assigned Distribution Statements B through X, per reference (g). Non-record copies may be shredded or torn into pieces and placed in trash containers. Records of destruction are not required.

2. Destroy Unclassified DEA Sensitive Information and NNPI in the same manner approved for classified information.

10-21 DISPOSITION OF CLASSIFIED INFORMATION FROM COMMANDS REMOVED FROM ACTIVE STATUS OR TURNED OVER TO FRIENDLY FOREIGN GOVERNMENTS

1. Commanding officers shall ensure that all classified information has been removed before relinquishing security control of a ship, shore activity, or aircraft for striking, decommissioning, deactivation, or rehabilitation. Disposal shall be per reference (g) or stored at an approved facility when the status is temporary.

a. The commanding officer shall certify to the command accepting custody that a security inspection has been conducted and that all classified information has been removed. If, for some reason, all classified information has not been removed, the certification shall document the information remaining, the authority and reason therefore.

b. Where possible, conduct the security inspection jointly with the command accepting custody.

2. Commanding officers shall ensure that the release of classified information in connection with the transfer to a friendly foreign government is processed per reference (m), and that the permission of the Archivist of the U.S. is obtained before transferring records to other agencies or non-U.S. Government organizations, including foreign governments, per reference (g).

REFERENCES

(a) DoD Instruction 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support*, 17 Feb 89 (NOTAL)

(b) OPNAVINST 5530.13B, *DON Physical Security Instruction for Conventional Arms, Ammunition and Explosives (AA&E)*, 5 Jul 94

(c) OPNAVINST 5112.5A, *Mail Handling and Delivery Procedures for Mailrooms and Postal Service Centers*, 17 Jun 87

(d) Title 18, U.S.C., Section 1386, *Crimes and Criminal Procedures*

(e) OPNAVINST 5530.14C, *DON Physical Security and Loss Prevention*, 10 Dec 98

(f) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(g) SECNAVINST 5212.5D, *Navy and Marine Corps Records Disposition Manual*, 22 Apr 98

(h) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(i) CMS-21 Series, *Interim CMS Policy and Procedures for Navy Tier 2 Electronic Key Management System*, 30 May 97 (NOTAL)

(j) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(k) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(l) NAVSO P-5239-26, *Remanence Security Guidebook*, Sep 93

(m) SECNAVINST 5510.34, *Manual for the Disclosure of DON Military Information to Foreign Governments and International Organizations*, 4 Nov 93

EXHIBIT 10A

VAULT AND SECURE ROOM (OPEN STORAGE AREA) CONSTRUCTION STANDARDS

1. VAULT

a. Floor and Walls. Eight inches of reinforced-concrete to meet current structural standards. Walls are to extend to the underside of the roof slab.

b. Roof. Monolithic reinforced-concrete slab of thickness to be determined by structural requirements, but not less than the floors and walls.

c. Ceiling. The roof or ceiling shall be reinforced-concrete of a thickness to be determined by structural requirements, but not less than the floors and walls.

d. Door. Vault door and frame unit shall conform to Federal Specification AA-D-2757, Class 8 vault door, or Federal Specification AA-D-600, Class 5 vault door. Doors shall be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740.

2. SECURE ROOM

a. Walls, Floor, and Roof. The walls, floor, and roof construction shall be of permanent construction materials; i.e. plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling with permanent construction materials, wire mesh, or 18-gauge expanded steel screen.

b. Ceiling. The ceiling shall be constructed of plaster, gypsum, wallboard material, hardwood, or any other acceptable material.

c. Doors. The access door to the room shall be substantially constructed of wood or metal and be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740. For open storage areas approved under previous standards, the lock may be the previously approved GSA combination lock until the door has been retrofitted with a lock meeting Federal Specification FF-L-2740. When double doors are used, an astragal will be installed on the active leaf of the door. The hinge pins of outswing doors shall be peened, brazed, or spot welded to prevent removal. Doors other than the access

door shall be secured from the inside (for example, by a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door, or by any other means that will prevent entry from the outside. Key operated locks that can be accessed from the exterior side of the door are not authorized). Each perimeter door shall be protected by a balanced magnetic switch that meets the standards of UL 634.

d. Windows. All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings. Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows shall be constructed from or covered with materials which provide protection from forced entry and shall be protected by an IDS, either independently or by the motion detection sensors in the space. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

e. Openings. Utility openings such as ducts and vents shall be kept at less than man-passable (96 square inches) opening. Openings larger than 96 square inches shall be hardened per the Military Handbook 1013/1A.

EXHIBIT 10B

PRIORITY FOR REPLACEMENT

Priorities range from 1 to 4, with 1 being the highest and 4 the lowest.

LOCK REPLACEMENT PRIORITIES IN THE U.S. AND ITS TERRITORIES

ITEM	TS/SAP	TS	S/SAP	S-C
Vault Doors	1	1	3	4
Containers(A)*	3	4	4	4
Containers(B)**	1	1	1	2
Crypto	1	1	2	2

LOCK REPLACEMENT PRIORITIES OUTSIDE THE U.S. AND ITS TERRITORIES

ITEM	TS/SAP	TS	S/SAP	S-C
Vault Doors	1	1	2	2
Containers(A)*	2	2	3	3
Containers(B)**	1	1	1	2
Crypto	1	1	2	2
High Risk Areas	1	1	1	1

*A-Located in a controlled environment where the DoD has the authority to prevent unauthorized disclosure of classified information. The U.S. Government may control or deny access to the space, post guards, require identification, challenge presence, inspect packages, program elevators, or take other reasonable measures necessary to deny unauthorized access.

**B-Located in an uncontrolled area without perimeter security measures.

EXHIBIT 10C

MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS OPTIONAL FORM 89

MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS

NOTE: Store this form in the security container or on the vault door.

TYPE ☐ SECURITY CONTAINER ☐ VAULT DOOR

SERIAL NUMBER (Containers: Located on the side of the control drawer. Vault Doors and Map and Plan Containers: Located on the inside face of the door.)

MANUFACTURER

GSA CLASS ☐ ONE ☐ TWO ☐ THREE ☐ FOUR ☐ FIVE ☐ SIX ☐ SEVEN

OPERATING PROBLEM	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN		ORGANIZATION NAME
			NAME	ACTIVITY	

SIGNATURE OF RESPONSIBLE OFFICIAL	NAME OF RESPONSIBLE OFFICIAL	DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION

OPTIONAL FORM 89 (9-98)

MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS
OPTIONAL FORM 89 (BACK)

OPERATING PROBLEM	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN		ORGANIZATION NAME
			NAME	ACTIVITY	

SIGNATURE OF RESPONSIBLE OFFICIAL	NAME OF RESPONSIBLE OFFICIAL	DATE SIGNED

OPTIONAL FORM 89 (9-98) BACK

EXHIBIT 10D

IDS AND ACCESS CONTROLS

1. **IDS.** An IDS must detect an unauthorized or authorized penetration in the secure area. An IDS complements other physical security measures and consists of the following:

a. Intrusion Detection Equipment (IDE)

b. Security forces

c. Operating procedures

2. **SYSTEM FUNCTIONS**

a. IDS components operate as a system with the following four distinct phases:

(1) Detection

(2) Reporting

(3) Assessment

(4) Response

b. These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.

(1) Detection: The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area to the Premise Control Unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise a "zone" at the monitor station.

(2) Reporting: The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. Another signal is added to the communication for supervision to prevent compromise of the communications scheme. The supervised signal is intended to disguise the information and protect the IDS against tampering or injection of false information by an intruder. The supervised signal is sent by the PCU through the transmission link to the monitor station. Inside the monitor station either a dedicated panel or central processor monitors information from the PCU

signals. When an alarm occurs, an annunciator generates an audible and visual alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

(3) Assessment: The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force.

(4) Response: The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response phase must also determine the precise nature of the alarm and take all measures necessary to safeguard the secure area.

3. THREAT, VULNERABILITY, AND ACCEPTABILITY

a. As determined by the commanding officer, all areas that reasonably afford access to the container, or where classified data is stored should be protected by an IDS unless continually occupied. Prior to the installation of an IDS, commanding officers shall consider the threat, vulnerabilities, in-depth security measures and shall perform a risk analysis.

b. Acceptability of Equipment: All IDEs must be UL-listed (or equivalent) and approved by the DoD Component or DoD contractor. Government-installed, -maintained, or -furnished systems are acceptable.

4. TRANSMISSION AND ANNUNCIATION

a. Transmission Line Security: When the transmission line leaves the secured area and traverses an uncontrolled area, Class I or Class II line supervision shall be used.

(1) Class I: Class I line security is achieved through the use of a data encryption system or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by the National Institute of Standards and Technology or another independent testing laboratory is required.

(2) Class II: Class II line supervision refers to systems in which the transmission is based on pseudo-random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a

minimum 6-month period. Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

b. Internal Cabling: The cabling between the sensors and the PCU should be dedicated to the IDE and must comply with national and local code standards.

c. Entry Control Systems: If an entry control system is integrated into an IDS, reports from the automated entry control system should be subordinate in priority to reports from intrusion alarms.

d. Maintenance Mode: When an alarm zone is placed in the maintenance mode, this condition should automatically signal to the monitor station and the IDS shall not be securable while in the maintenance mode. The alarm or message must be continually visible at the monitor station throughout the period of maintenance. A standard operating procedure must be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods shall be archived in the system. A self-test feature shall be limited to 1 second per occurrence.

e. Annunciation of Shunting or Masking Condition: Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

f. Alarms Indications: Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the secure area.

g. Power Supplies: Primary power for all IDE shall be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment shall change power sources without causing an alarm indication.

(1) Emergency Power: Emergency power shall consist of a protected independent backup power source that provides a minimum of 4-hours operating power battery and/or generator power. When batteries are used for emergency power, they shall be maintained at full charge by automatic charging circuits. The manufacturer's periodic maintenance schedule shall be followed and results documented.

(2) Power Source and Failure Indication: An illuminated indication shall exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station shall indicate a failure in power source, and the location of the failure or change.

h. Component Tamper Protection: IDE components located inside or outside the secure area shall be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection shall be provided.

5. SYSTEM REQUIREMENTS

a. Independent Equipment: When many alarmed areas are protected by one monitor station, secure room zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

b. Access and/or Secure Switch and PCU: No capability should exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs must be located inside the secure area and should be located near the entrance. Assigned personnel should initiate all changes in access and secure status. Operation of the PCU may be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

c. Motion Detection Protection: Secure areas that reasonably afford access to the container or where classified information is stored should be protected with motion detection sensors (e.g., ultrasonic and passive infrared). Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector shall cause an immediate and continuous alarm condition.

d. Protection of Perimeter Doors: Each perimeter door shall be protected by a balanced magnetic switch that meets the standards of UL 634.

e. Windows: All readily accessible windows (within 18 feet of ground level) shall be protected per appendix 10A.

f. IDS Requirements for Continuous Operations Facility: A continuous operations facility may not require an IDS. This type

of secure area should be equipped with an alerting system if the occupants cannot observe all potential entrances into the room. Duress devices may also be required.

g. False and/or Nuisance Alarm: Any alarm signal transmitted in the absence of a detected intrusion or identified as a nuisance alarm is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. All alarms shall be investigated and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms should not exceed one in a period of 30 days per zone.

6. INSTALLATION, MAINTENANCE, AND MONITORING

a. Installation and Maintenance Personnel: Alarm installation and maintenance should be accomplished by U.S. citizens who have been subjected to a trustworthiness determination per SECNAVINST 5510.30A.

b. Monitor Station Staffing: The monitor station shall be supervised continuously by U.S citizens who have been subjected to a trustworthiness determination per SECNAVINST 5510.30A.

7. ACCESS CONTROLS. The perimeter entrance should be under visual control at all times during working hours to prevent entry by unauthorized personnel. This may be accomplished by several methods (e.g., employee work station, guard CCTV). Regardless of the method used, an ACS shall be used on the entrance. Uncleared persons are to be escorted within the facility by a cleared person who is familiar with the security procedures at the facility.

a. Automated Entry Control Systems (AECS): An automated entry control system may be used to control admittance during working hours instead of visual control, if it meets the AECS criteria stated in subparagraphs 7.a and b below. The AECS must identify an individual and authenticate the person's authority to enter the area through the use of an identification badge or card.

(1) Identification Badges or Key Cards. The identification badge or key card must use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) Personal Identity Verification: Personal identity verification (Biometrics Devices) identifies the individual requesting access by some unique personal characteristic, such as:

(a) Fingerprinting

(b) Hand Geometry

(c) Handwriting

(d) Retina scans

(e) Voice recognition

A biometrics device may be required for access to the most sensitive information.

b. In conjunction with subparagraph 7.a(1) above, a personal identification number (PIN) may be required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

c. Authentication of the individual's authorization to enter the area must be accomplished within the system by inputs from the identification badge/card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer, or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than the required access level.

d. Protection must be established and maintained for all devices or equipment which constitute the entry control system. The level of protection may vary depending upon the type of device or equipment being protected.

(1) Location where authorization data and personal identification or verification data is input, stored, or recorded must be protected.

(2) Card readers, keypads, communication or interface devices located outside the entrance to a controlled area shall

have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.

(3) Keypad devices shall be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

(4) Systems that use transmission lines to carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area shall have line supervision.

(5) Electric strikes used in access control systems shall be heavy duty, industrial grade.

e. Access to records and information concerning encoded identification data and PINs shall be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system shall be limited to the fewest number of personnel as possible. Such data or software shall be kept secure when unattended.

f. Records shall be maintained reflecting active assignment of identification badge/card, PIN, level of access, and similar system-related records. Records concerning personnel removed from the system shall be retained for 90 days. Records of entries shall be retained for at least 90 days or until investigations of system violations and incidents have been investigated, resolved, and recorded.

g. Personnel entering or leaving an area shall be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirmation of need-to-know and access. The Heads of DoD components may approve the use of standardized AECS which meet the following criteria:

(1) For a Level 1 key card system, the AECS must provide a .95 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.05 probability after three attempts to gain entry.

(2) For a Level 2 key card and PIN system, the AECS must provide a 0.97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.010 probability after three attempts to gain entry have been made.

(3) For a Level 3 key card and PIN and biometrics identifier system, the AECS must provide a 0.97 probability of granting access to an unauthorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.005 probability after three attempts to gain entry have been made.

h. Electric, Mechanical, or Electromechanical Access Control Devices: Electric, mechanical, or electromechanical devices which meet the criteria stated below may be used to control admittance to secure areas during duty hours if the entrance is under visual control. These devices are also acceptable to control access to compartmented areas within a secure area. Access control devices must be installed in the following manner:

(1) The electronic control panel containing the mechanical mechanism by which the combination is set is to be located inside the area. The control panel (located within the area) will require only minimal degree of physical security designed to preclude unauthorized access to the mechanism.

(2) The control panel shall be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.

(3) The selection and setting of the combination shall be accomplished by an individual cleared at the same level as the highest level of classified information controlled within.

(4) Electrical components, wiring included, or mechanical links (cables, rods, etc.) should be accessible only from inside the area, or, if they traverse an uncontrolled area they should be secured within protecting covering to preclude surreptitious manipulation of components.